

# STORAGE SWITZERLAND BRIEFING REPORT

## MAINTAINING CONFIDENCE - HOW THE DPSM PROCESS MANAGES PROBLEMS



Eric Slack, Senior Analyst

Data protection is effectively insurance against data loss and breakdowns in business continuity. And like insurance, a data protection system should provide confidence that these risks are reduced to an acceptable level. This confidence comes from having a comprehensive data protection services management system in place and knowing it's working - not from simply running a backup application. But how does this system maintain confidence when something does go wrong - a backup job fails or a restore doesn't complete in time to meet business objectives, for example? And how does the system maintain its effectiveness through the day to day infrastructure changes that occur in the modern data center?

After the data protection system is up and running, how do you fix issues that come up?

As the old saying goes, "an ounce of prevention is worth a pound of cure" - but things do go wrong. Backup jobs fail, they run past the established backup window, a restore doesn't provide the data expected, in the timeframe expected, etc. How does the data protection system support problem resolution quickly and identify root causes, to assure that any needed changes to the system are made and the same problem isn't 'fixed' again?

In addition to fixing current problems, how do you make sure the data protection process is up to date so that changes to the environment don't cause more problems in the future? Modern IT environments are dynamic with new applications, platforms, storage, users, etc., forcing continual configuration changes to the data protection system. These changes can have real impact on SLAs and need to be tracked and managed.

Data protection is a cost center, not a source of revenue. And, pressure to contain those costs are ever-present, along with expectations of improved performance to end-user customers. How do you get operational improvements and cost reduction in parallel with maintaining confidence?

Effective problem resolution

The first step is to identify the SLA impact of the problems presented and prioritize the responses to them, basically, fix the most important problems first. A Data Protection Services Management (DPSM) system, like [Bocada's Prism](#), is able to help users determine the SLA impact of a backup error and have alarms that are triggered by the most critical events automatically. Then, next actions can be prioritized, whether that's immediate corrective action, further analysis, etc. It also may determine that some events don't need a response.

The process of troubleshooting and identifying root cause and resolution should also be as efficient as possible. This requires navigation according to the workflow the user follows, stepping through tasks the same way the user does. Following an operational process, instead of the 'wormhole' experience of jumping between views and screens, makes it easier to recreate problems and see what actually happened.

Steps taken and reasons for failure should be annotated, directly, and attached to the job or client/server, allowing others to work the same problem event and making handling a similar problem easier next time it comes up. These notes could be emailed to management, customers or other support personnel as needed, facilitating problem escalation by bringing new people up to speed faster. This can improve customer satisfaction and reduce the workload on IT which often must produce regular status updates for stakeholders. These annotations can also be used to develop a Knowledge Base to assure that everything that can be learned from the experience has been captured and to provide data efficiently in response to audits.

#### Management vs Monitoring - Updating the DPSM process

Overall, IT needs management of SLA compliance, not just monitoring of backup tasks. Monitoring assumes what you're observing is valid and will provide useful information. Management doesn't make that assumption - it validates the data being gathered as effective at producing desired results. This validation comes from constantly updating policies and procedures to assure that they're current with changing business needs. Schedule or policy changes should be tracked and trigger notification and review of their affects on backup success rates. Similarly, proactive SLA impact and trending reports can show how policy or infrastructure changes may affect SLAs and *why* an SLA isn't being met.

#### Improving operational effectiveness

In addition to fixing problems, regular system improvements should be part of the DPSM solution. These improvements can be subjective, like increased user satisfaction, management confidence or IT peace of mind. They can also be objective, like CapEx and OpEx reductions.

Confidence and satisfaction are a direct result of communication. Having reports emailed directly from within the system when a remediation action is taken can assure end users that their issue is being resolved. Similarly, providing regular status updates during the remediation process can maintain stakeholders' confidence.

CapEx savings can result from infrastructure improvements and lowered capacity costs by eliminating redundant backup jobs and better utilizing media. Through the use of chargebacks, user-customers often become more efficient and help drive down infrastructure costs as well. On the OpEx side, efficient troubleshooting and annotation means faster problem resolution and reduced support time and issue escalation. Automated reporting, policy and SLA management reduces IT admin time required to maintain and manage the data protection process, while providing more complete information to management and end-user customers.

A Data Protection Services Management system, like Prism, can provide confidence that an organization's data is protected and its business-critical services are supported at acceptable levels. These systems align data protection tasks with appropriate SLAs and provide assurance to stakeholders that effective processes are in force in case of a failure. When a failure does occur, they assess its impact on SLAs and prioritize an appropriate response. As the IT infrastructure evolves, the DPSM system tracks the configuration and policy changes that affect SLAs and enables IT to manage them proactively. This ongoing process to maintain confidence can also produce improvements in operational efficiency and lower costs.

### **About Storage Switzerland**

**Storage Switzerland is an analyst firm focused on the virtualization and storage marketplaces. For more information please visit our web site: <http://www.storage-switzerland.com>**

*Copyright © 2011 Storage Switzerland, Inc. - All rights reserved*